



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

50

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/826,310	04/03/2001	Douglas M. Winneg	S01400/70001DPM	4169

23628 7590 06/14/2005

WOLF GREENFIELD & SACKS, PC  
FEDERAL RESERVE PLAZA  
600 ATLANTIC AVENUE  
BOSTON, MA 02210-2211

EXAMINER
----------

ARANI, TAGHI T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 06/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/826,310

Applicant(s)

WINNEG ET AL.

Examiner

Taghi T. Arani

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 3/2/4/2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-8,10-22,24-36,38-50,52-65,67-81 and 83-90 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) \_\_\_\_\_ is/are rejected.
- 7) ☒ Claim(s) 1-8,10-22,24-36,38-50,52-65,67-81,83-90 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

Art Unit: 2131

**DETAILED ACTION**

**DETAILED ACTION**

1. Claims 1-8, 10-22, 24-36, 38-50, 52-65, 67-81, 83-90 are pending for examination.

**Response to Amendment**

2. Applicant's amendment and arguments filed 3/2/4/2005 necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 53 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 53 recites the limitation "'act (B)(1)" in line 1. There is insufficient antecedent basis for this limitation in the claim. For purpose of applying art, the Examiner assumes "act (B)"

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-8, 10-22, 24-36, 38-50, 52-65, 67-81, 83-90 are rejected under 35 U.S.C. 102(a) as being anticipated by WO 99/36848 published July 1999 and further in view of U.S. Patent 6,266,73 to Kisor et al. (hereinafter "kisor").

**As per claims 1, 44, 57,59, 74 and 88**, WO 99/36848 from EXAMSOFT WORLDWIDE INC. (hereinafter "EXAMSOFT") teaches a method/apparatus of securely executing on a computer system an application for receiving, from a user of the computer system, at least one response to at least one question of an examination, the computer system comprising an input device and a display device for displaying content to the user, the method comprising acts of [abstract]:

(A) executing the application on the computer system, comprising displaying an area on the display device in which the user can enter a response to at least one question of the examination, and enabling the user to use the input device to input a response for one or more of the questions into the displayed area [page 2, lines 5-8, Fig. 1, page 9, lines 14-17]; and

(B) prohibiting the computer system from accessing any unauthorized content during execution of the application and from displaying any authorized content to the user during execution of the application [page 2, lines 8-19, i.e. executable instructions for closing unauthorized programs and filtering user commands to prevent unauthorized access to files stored on the computer].

While EXAMSOFT discloses detecting unauthorized processes executing during the displaying of the area on the display device [ EXAMSOFT (abstract) discloses a method and computer program provided for creating a secure computing environment by preventing access

Art Unit: 2131

to unauthorized files during the execution of a desired application. User commands are filtered for instructions that would lead to unauthorized application (process) access. This restricts access to all files except the file created by the desired application , emphasis added].

EXAMSOFT fails to teach ( as persuasively argued by the Applicant ) terminating (detected) unauthorized processes executing during the displaying of the area on the display device.

However, Kisor teaches detecting and determining any unauthorized processes executing during the displaying of the area on the display device [ Kisor teaches ( col. 3, line 42 through col. 4, line 3) “ When event detector 40 detects an event on event list 46, decision maker 42 determines whether the event is permitted. Permission category list 48 lists permission categories for different events. Action generator 44 then accesses action list 50 to determine the appropriate action for the permission category found in permission category list 48 for the detected event. Exemplary action includes permitting the event, denying the event, killing the process (i.e., preventing present and future executions, until a predetermined reset occurs), locking down the computer by shutting down the processor while maintaining the memory, activating an alarm, and reporting the event. A report might be stored in memory for later retrieval (see exemplary FIG. 6's, "security log/report") or sent to a system administrator, to a security office, to other users of the network, or to any other recipient who might use the report of the event. As one example with respect to FIG. 6, suppose that a user X attempts the event of "access password list file." User X only has a "permission category=2" designation, whereas the attempted event has a permission category list 48 designation of category "3". Therefore the computer system detects unauthorized activity, and action generator 44 performs the action list 50 actions of "D" (denying

Art Unit: 2131

the activity), "R" (reporting the activity) (see FIG. 6's security log/report) and "A" (issue an alarm, such as a prompt to a display screen or audible output from a speaker). A similar unauthorized activity can be detected if a program, e.g., e-mail "program Z", suddenly attempts to access and then e-mail private accounting files back onto the internet.], emphasis added by the Examiner.

Therefore, It would have been obvious to one of ordinary skill in the art to modify EXAMSOFT's invention with the teaching of Kisor et al's computer security system to not only restrict access to the secure contents in EXAMSOFT's secure exam system, but also to take other necessary action in response to detection of an unauthorized process [col. 1, lines 29-37, see also Fig. 2, elements 46, 48 and 50 ( Kisor)].

**As per claims 2, 58, 75 and 89**, EXAMSOFT teaches the method/apparatus of claims 1, 44 and 74 respectively, wherein act (A) further comprises an act of displaying the at least one question of the examination on the display device [page 4, lines 3-5, i.e. the exam application's own easy to use word processor, page 9, lines 14-17, i.e. multiple choice examination].

**As per claim 3, 45, 60 and 76**, EXAMSOFT teaches the method/apparatus of claims 1, 44, 59 and 74 respectively, wherein prior to performance of act (A), one or more unauthorized processes are executing on the computer system [page 7, lines 21-22, i.e. identifying already running processes], wherein act (B) comprises an act of terminating the one or more unauthorized processes prior to performing act (A) [page 8, lines 6-10, i.e. unauthorized processes are either closed or hidden].

**As per claim 4, 46, 61 and 77**, EXAMSOFT teaches the method/apparatus of claims 1, 44, 59 and 74 respectively, wherein act (B) comprises an act of (1) configuring the application

Art Unit: 2131

such that unauthorized content cannot be accessed by the application [page 8, lines 10-16, lines 18-19, i.e. configuring the Windows for optimum security].

**As per claim 5, 47, 62 and 78**, EXAMSOFT teaches the method/apparatus of claims 4, 46, 61 and 77 respectively, wherein act (B)(1) comprises an act of configuring the application such that unauthorized processes cannot be initiated by the application [page 8, i.e. updating the .INI files to reflect the changes made by the exam application such as terminating or hiding the Explorer windows].

**As per claims 6, 48, 63 and 79**, EXAMSOFT teaches the method/apparatus of claims 1, 44, 59 and 74 respectively, wherein act (B) comprises an act of (1) prior to executing act (A), disabling any functions on the computer system capable of performing at least one of the following: accessing unauthorized content and displaying unauthorized content to a user of the computer system [page 8, lines 18-20, i.e. the exam application terminates or hides Explorer and turns off screen savers, power management, the desktop wall paper, sets the desktop icons invisible ].

**As per claim 7, 49, 64 and 80**, EXAMSOFT teaches the method/apparatus of claims 6, 48, 63 and 79 respectively, wherein act (B)(1) comprises an act of disabling any functions on the computer system that are capable of initiating unauthorized processes on the computer system [page 8, lines 22-23, i.e. disabling the task bar in WIN9x and NT versions]

**As per claim 8, 50, 65 and 81**, EXAMSOFT teaches the method of claims 1, 44, 63 and 79 respectively, wherein act (B)(1) comprises an act of configuring one or more programming hooks of the computer system [page 9, lines 1-4].

**As per claims 10, 52, 67 and 83**, EXAMSOFTEACHES the method/apparatus of claims 1, 55, 59 and 74 respectively, further comprising:

recording each detection of an unauthorized process [page 10, lines 9-15, i.e. test taking statistics and storing in an auxiliary information file].

**As per claims 11, 53, 68 and 84**, EXAMSOFTEACHES the method/apparatus of claims 9, 51, 59 and 79 respectively, wherein act (B)(1) comprises acts of (a) detecting any processes executing on the computer system during execution of the application [page 9, lines 5-12, lines 19-23 i.e. setting hooks and monitoring all keystrokes and other user input as the examination proceeds]. (b) for each detected process, determining if the detected process is authorized to execute on the computer system during execution of the application [page 9, lines 20-22, i.e. the Exam application records the details of all intercepted hooked messages, such as attempts to call unauthorized applications or access unauthorized data],and

While EXAMSOFTEACHES disclosing intercepting messages and determining whether the messages would lead to access of an unauthorized file and modifies those intercepted messages that would lead to access of an unauthorized file( page 13, claim19a) , i.e. closing undesired processes running on the computer.

EXAMSOFTEACHES does not disclose (c) for each detected process, if the detected process is unauthorized, terminating the detected process.

However, Kisor teaches for each detected process, if the detected process is unauthorized, terminating the detected process [col. 3, line 42 through col. 4, line 3].

Therefore, It would have been obvious to one of ordinary skill in the art to modify EXAMSOFTEACHES's invention with the teaching of Kisor et al's computer security system to not only



restrict access to the secure contents in EXAMSOFT's secure exam system, but also take other necessary action in response to detection of an unauthorized process [col. 1, lines 29-37, see also Fig. 2, elements 46, 48 and 50 (Kisor)].

**As per claims 12, 54, 69 and 85**, EXAMSOFT as modified teach the method/apparatus of claims 11, 53, 68 and 84 respectively, wherein the computer system comprises a registry that lists all processes currently executing on the computer system [page 7, lines 21-25], and act (B)(1)(a) comprises an act of periodically accessing the registry on the computer system at predefined intervals to ascertain the processes currently executing on the computer system [page 10, lines 4-19].

**Claims 15-26** are apparatus claims corresponding to method claims 1-8, 10-12. Claims 15-26 are rejected for the same reasons provided in the statement of rejections of claims 1-8, 10-12 above.

**Claims 29-36 and 38-40** are apparatus claims corresponding to the method claims 1-8, 10-12. Claims 29-36, and 37-40 are rejected for the same reasons provided in the statement of rejections of claims 1-8, 10-12 above.

**Claims 43 and 90** are computer program products corresponding to the method claims 1 and 74 respectively. Claims 43 and 90 are rejected for the same reasons stated in the statement of rejections of claims 1 and 74 above.

**As per claims 13 and 14**, While EXAMSOFT discloses detecting unauthorized processes executing during the displaying of the area on the display device [ EXAMSOFT (abstract) discloses a method and computer program provided for creating a secure computing environment by preventing access to unauthorized files during the execution of a desired

Art Unit: 2131

application. User commands are filtered for instructions that would lead to unauthorized application (process) access. This restricts access to all files except the file created by the desired application , emphasis added].

EXAMSOFT fails to teach:

(C) managing a list of unauthorized processes, wherein act (B)(1)(b) comprises an act of, for each detected process, comparing the detected process to the list of unauthorized processes, and wherein act (B)(1)(c) comprises, for each detected process, terminating the detected process if the detected process is on the list.

(C) managing a list of processes authorized to be executed on the computer system, wherein act (B)(1)(b) comprises an act of, for each detected process, comparing the detected process to the list of authorized processes, and wherein act (B)(1)(c) comprises, for each detected process, terminating the detected process if the detected process is not on the list.

However, Kisor et al. teach a computer security system and method wherein an event detector detects events (i.e. processes) occurring in a monitored computer system [abstract].

Kiser et al teach managing a list of unauthorized processes and a list of processes authorized to be executed on the computer system comprises an act of, for each detected process, comparing the detected process to a list of unauthorized processes and comparing the detected process to a list of authorized processes [col. 2, lines 54-67].

Kiser et al. further teach an action generator to determine an appropriate action [such as killing the process, col. 3, lines 42-50, such as terminating the detected process].

It would have been obvious to one of ordinary skill in the art to modify EXAMSOFT's invention with the teaching of Kisor et al's computer security system to not only restrict access

Art Unit: 2131

to the secure contents in EXAMSOFT's secure exam system, but also to take other action in response to detection of an event [col. 1, lines 29-37, see also Fig. 2, elements 46, 48 and 50 (Kisor et al.)].

**Claims 27-28, 41-42, 55-56, 70-71 and 86-87** are apparatus claims corresponding to the method claims 13-14. Claims 27-28, 41-42, 55-56, 70-71 and 86-87 are also rejected for the same reasons stated in the statement of rejections of claims 13-14 above.

### **Action is Final**

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

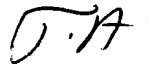
### **Conclusion**

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

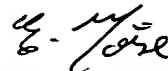


Taghi T. Arani, Ph.D.

Examiner

Art Unit 2131

6/9/05



**EMMANUEL L. MOISE**  
**SUPERVISORY PATENT EXAMINER**